

# Incident Management

---

## Description

Incident management is the performance of reactive and proactive services to help prevent and handle computer security events and incidents. It is broader than the traditional views of incident response handled by an individual person, team, or group (an IT department, for example). The scope of this definition of incident management is preventing and handling computer security incidents. It includes identifying and minimizing the impact of technical vulnerabilities in software or hardware that may expose computing infrastructures to attacks or compromise, thereby causing incidents. Because of the variety of ways that incident management capabilities can be organized and staffed, a starting point for building an incident management functional model has been to document the processes involved in effective and efficient incident management work, regardless of where they occur across an organization or enterprise.

## Overview Articles

Name	Version Creation Time	Abstract
Incident Management	24/04/06 15:59:21	A computer security incident management capability is the ability to provide management of computer security events and incidents. It implies end-to-end management for controlling or directing how security events and incidents should be handled. This involves defining a process to follow with supporting policies and procedures in place, assigning roles and responsibilities, having appropriate equipment, infrastructure, tools, and supporting materials ready, and having qualified staff identified and trained to perform the work in a consistent, high-quality, and repeatable way.

## Most Recently Updated Articles [Ordered by Last Modified Date]

Name	Version Creation Time	Abstract
Incident Management	24/04/06 15:59:21	A computer security incident management capability is the ability to provide management of computer security events and incidents. It implies end-to-end

		management for controlling or directing how security events and incidents should be handled. This involves defining a process to follow with supporting policies and procedures in place, assigning roles and responsibilities, having appropriate equipment, infrastructure, tools, and supporting materials ready, and having qualified staff identified and trained to perform the work in a consistent, high-quality, and repeatable way.
--	--	---

## All Articles [Ordered by Title]

Name	Version Creation Time	Abstract
Incident Management	24/04/06 15:59:21	A computer security incident management capability is the ability to provide management of computer security events and incidents. It implies end-to-end management for controlling or directing how security events and incidents should be handled. This involves defining a process to follow with supporting policies and procedures in place, assigning roles and responsibilities, having appropriate equipment, infrastructure, tools, and supporting materials ready, and having qualified staff identified and trained to perform the work in a consistent, high-quality, and repeatable way.

## Fields

Name	Value
Categories	best-practices